HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/582,797	09/06/2000	Claude Meggle	15675.P321	2849

7590 05/17/2005

Blakely Sokoloff Taylor & Zafman
7th Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 05/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/582,797	**Applicant(s)** MEGGLE, CLAUDE	
	Examiner Thanhnga B. Truong	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 03/03/2005 (RCE).

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 17-26 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 17-26 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 29 June 2000 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Applicant's submission for RCE filed on March 03, 2005 has been entered.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 17-20 and 22-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powers (US 5,655,020), and further in view of Henry (US 4,399,323).

a. Referring to claim 17:

i. Powers teaches:

(1) receiving a confidential code inputted by a user **[i.e., receiving a first code comprising a plurality of characters in sequential positions identifying the authorized person (column 2, lines 44-45)];**

(2) verifying a first user entitlement by performing the comparison process on said confidential code **[i.e., as shown in Figure 2a, step 20 is to look up, that is "to verify" pin 1, that is, "determined by a first code"];**

(3) if said first user entitlement is recognized, allowing access of the user to a first secure functionality **[as shown in Figure 2a, step 20a found decision can include "if said first user entitlement is recognized, allowing access of the user to a first secure functionality"];** and

(4) if said entitlement is not recognized, converting said inputted code into an alternate code by applying said reverse conversion scheme, verifying a second user entitlement by performing said comparison process on said alternate confidential code **[i.e., receiving a second code comprising a plurality of characters in sequential positions obtained from an actual user; comparing the characters of the second code with the characters in corresponding positions of**

the first code to determine identity between the codes in all but one of the character positions (column 2, lines 46-51)];

(5) if said second entitlement is recognized, allowing access of the user to a second functionality which is restricted relative to said first secure functionality without providing any information on the fact that the inputted code failed to provide entitlement **[i.e., receiving a second code comprising a plurality of characters in sequential positions obtained from an actual user, the second code having more characters than the first code; comparing the characters of the second code with the characters of the first code to determine whether the second code contains a sequence of characters in the same order as the sequence in the first code (column 3, lines 15-21)];**

ii. However, Power does not explicitly mention:

(1) providing a conversion scheme that a starting code to be converted into a converted code for a user to convert their confidential code into an emergency code, said conversion scheme having a reverse conversion scheme to convert said converted code into said starting code;

iii. Whereas, Henry teaches:

(1) by further enciphering a received enciphered message with a private enciphering key. The doubly enciphered message is then deciphered with a private deciphering key into the original message. **(column 1, lines 38-41 of Henry).** Furthermore, in Figure 4, enciphering device 21 is shown including transmission gate array 40, accumulator 41 and reduction modulo-M circuit 42. Enciphering device 21 responds to private enciphering key A and modulus M for transforming enciphered message S.sub.H into a different enciphered message S.sub.E. Message S.sub.E is actually doubly encrypted because it contains the public enciphering key H employed to generate S.sub.H as well as the private enciphering key A obtained during enciphering in device 21 **(column 6, lines 17-26 of Henry).**

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) combine the teaching of Henry into Power's system because as the required amount of privacy increases, the transmission rate for encrypted data messages decreases because of an increased complexity of decryption. **(column 1, lines 14-17 of Henry).**

v. The ordinary skilled person would have been motivated to:

(1) combine the teaching of Henry into Power's system since public key cryptographic systems afford authorized users a private means of communication even though unauthorized parties may intercept all of the communication. Heretofore, data transmission rates for these public key cryptographic systems have been constrained to be less than several kilobits per second because of decryption complexity **(column 1, lines 24-30 of Henry).**

b. *<u>Referring to claims 18 and 23:</u>*

i. Powers teaches:

(1) wherein said conversion scheme consists in shifting by a unit a given character on the starting code **[i.e., a user will be instructed to deliberately alter one character in his personal identification number before he uses it (column 3, lines 48-50)].**

c. *<u>Referring to claims 19 and 24:</u>*

i. Powers teaches:

(1) wherein said second functionality comprises displaying a message on a display of the system, said message simulating a failure in a tentative access to the first secure functionality **[i.e., as shown in Figure 2a, at step 21, the length of the PIN (PIN 2) offered by the user is compared with the authentic PIN (PIN 1) and if the number of characters is not the same the transaction is rejected, wherein the displaying a message is inherently provided. (column 5, lines 59-62). Furthermore, as one example of "banking transaction secure", the retailer then enters the version of the personal identification number offered by the customer into the computer system and awaits an authentication or invalid signal. Alternatively, the customer enters the number himself. If the version of the personal identification number which has been offered differs from**

the correct personal identification number according to a predetermined corruption algorithm and if that version of the personal identification number has not already been used within a predetermined time period the computer system will indicate that the user is authenticated. In other circumstances the computer system will produce a transaction invalid signal and this will prompt the retailer to ask further questions of the customer concerning personal details relating to the permitted user of the card (column 5, lines 15-28)].

d. *Referring to claims 20 and 25:*

i. Powers teaches:

(1) wherein said first secure functionality is a banking transaction and said system is a bank card terminal **[i.e., in step 20 data is derived from a credit card offered for use (or making bank transaction) via the magnetic stripe reader 2, that is, "at a bank card terminal", and is passed to the controller 8 to cause the PIN (PIN 1) associated with the permitted user of that credit card to be located (column 5, lines 51-55)].**

e. *Referring to claim 22:*

i. This claim consist a system to implement claim 17 and is rejected by the same prior art of record.

f. *Referring to claim 26:*

i. This claim has limitation that is similar to those of claim 17, thus it is rejected with the same rationale applied against claim 17 above.

4. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Powers, and further in view of Henry and Lichty (US 4, 774,500).

a. *Referring to claim 21:*

i. Powers and Henry teach the claimed subject matter except for:

(1) wherein said conversion scheme is variable depending on other data of said portable card (or microprocessor card).

ii. Lichty teaches:

(1) when the microprocessor cards are issued to individual users, a validation procedure is executed on a validating terminal. The procedure generally requires the issuer to enter the correct manufacturers' assigned key number in order to confirm that the card is authorized. A PIN is then assigned to or selected by the cardholder and stored in the secret zone. Upon completion of the validation procedure, the card MPU irreversibly alters its program so that the words written in the secret memory zone cannot be altered. Thereafter, upon using the card, a user must enter the correct PIN in order to confirm that the card is being used by its authorized user **(column 6, lines 65-68 through column 7, lines 1-9 of Lichty).**

(2) a useful development in account cards has been to incorporate a magnetic, semiconductor, or optically written memory for storing account information, current balances, or other user information in the card itself **(column 1, 26-29).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) apply such microprocessor card in Power/Henry's recited elements because such memory cards allow the user to access distributed terminals for off-line transactions, by reading and/or updating the stored information, without needing to have the transaction validated through a central system **(column 1, lines 30-34 of Lichty).**

iv. The ordinary skilled person would have been motivated to:

(1) include such microprocessor card in Power/Henry's recited elements since account cards having on-board memories can be made secure against data tampering by using a storage medium which is non-erasable, i.e. data is written once on the card and cannot be erased or changed **(column 1, lines 39-42 of Lichty).**

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Gutowitz (US 5, 365, 589) discloses encryption continues over a plurality of cycles. During each cycle the current keys are applied either backward or forward in time to their current states, over a plurality of sub-cycles. If during an encryption cycle an irreversible dynamical system is iterated in the backward direction, the choice of antecedent states may either be made randomly or according to information from the input information stream. After all encryption cycles have been performed, the current states of the dynamical system constitute the ciphertext. The ciphertext may then be decrypted by a method similar to the encryption method (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

AU 2135

TBT
May 10, 2005